Sony Ericsson

SO-01B
（Android OS 2.1用）

VPN（仮想プライベートネットワーク）展開ガイド

2010 年 10 月　第 1 版

A-DV6-100-01(1)

目次

このガイドはシステム管理者用です。SO-01BのVPN機能を利用するための設定について説明します。

概要

VPN（Virtual Private Network）により、公衆の無線LANホットスポットや自宅のインターネット回線などを専用回線のように使用することで、外出先からの企業内へのセキュアなネットワーク接続を実現することが可能です。これにより、企業内のファイルサーバー、メールサーバー、WEBコンテンツなどのリソースに対して、安全にアクセスすることができます。
VPN機能を使用する際は、セキュリティに関して十分な知識を持った管理者の指導のもとご利用ください。万一、適切な設定が行われないままVPN機能を使用した場合、十分なセキュリティが確保されませんので、ご注意ください。

VPNプロトコル

SO-01Bでは次のVPNプロトコルをサポートしています。

VPNプロトコル	説明
PPTP	Point to Point Tunneling Protocol
L2TP	Layer 2 Tunneling Protocol
L2TP/IPSec PSK	Layer 2 Tunneling Protocol / IP Security with Pre-shared key
L2TP/IPSec CRT	Layer 2 Tunneling Protocol / IP Security with Certificate

PPTP

MPPEによる暗号化が利用可能です。暗号化を利用する場合は、ユーザー認証方式を暗号化対応のプロトコルとしてMS-CHAPまたはMS-CHAPv2を選択する必要があります。

L2TP

事前共有鍵による、機器認証に対応しています。

L2TP/IPSec PSK

事前共有鍵による、機器認証に対応しています。IPSecによる暗号化が利用可能です。

L2TP/IPSec CRT

証明書による、機器認証に対応しています。よりセキュアな運用が可能です。

VPNプロトコルとそれぞれの認証・暗号化の組み合わせは以下の通りです。

VPNプロトコル	パケット認証	機器認証	暗号化	ユーザー認証
PPTP	—	—	暗号化なし、MPPE(RSA RC4 40bit,128bit)	MS-CHAPv2, MS-CHAP, CHAP, PAP
L2TP	—	事前共有鍵	—	
L2TP/IPSec PSK	AH, ESP	事前共有鍵	暗号化なし、DES, Triple-DES, AES	
L2TP/IPSec CRT	AH, ESP	証明書	暗号化なし、DES, Triple-DES, AES	

IKEプロポーザル

SO-01Bが対応するIKEプロポーザルは次の通りです。

種別	値
DH Group	2(1024bit)
ISAKMP hash	MD5, SHA1
ISAKMP HMAC hash	HMAC-MD5, HMAC-SHA1
ISAKMP encryption	DES-CBC, 3DES-CBC, AES-CBC-128
IPSec encryption	DES-CBC, 3DES-CBC, AES-CBC-128
IPSec HMAC hash	HMAC-MD5, HMAC-SHA1

SO-01BのVPN設定と接続

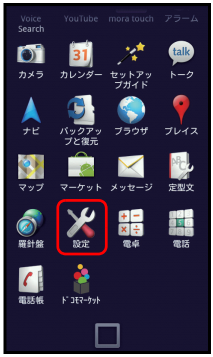
ここでは、SO-01BでのVPN設定方法と接続方法を説明します。この手順を繰り返すことで、複数のVPN接続プロファイルを作成し保存することもできます。

VPNの構成と保存

SO-01BにてVPN構成を作成・変更・削除するときは、SO-01Bのアプリケーション画面より、「設定」→「無線とネットワーク」→「VPN設定」とタップします。VPN構成を作成するときは「VPNの追加」をタップしたあと、使用するVPNプロトコルをタップします。また、既存の構成を変更または削除するときは一覧に表示されているVPN名を長くタッチします。

1　アプリケーション画面で「設定」をタップする

設定画面が表示されます。ホーム画面にて を押したあと「設定」をタップすることによっても同じ操作が可能です。



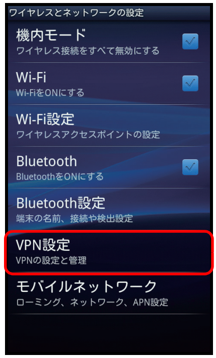
2　設定画面で「無線とネットワーク」をタップする

ワイヤレス設定画面が表示されます。



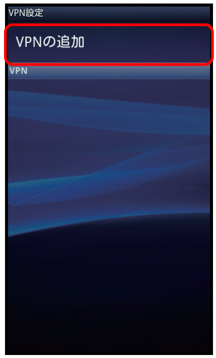
3 ワイヤレスとネットワークの設定画面で「VPN設定」をタップする

VPN設定画面が表示されます。



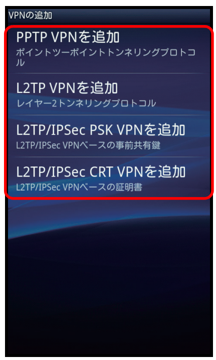
4 VPN設定画面で「VPNの追加」をタップする

VPNの追加画面が表示されます。



5 追加するVPNの種類をタップする

VPN詳細設定画面が表示されます。次項を参考にVPN構成の値を設定してください。



■ PPTP VPN設定

PPTP VPNの追加をタップしたときは、次のような画面が表示されます。



次の表に従って値を設定します。

項目名	説明
VPN名	このVPN構成の任意の名称を設定します。
VPNサーバーの設定	VPNサーバーのFQDNまたはIPアドレスを設定します。
暗号化を無効にする	MPPE(Microsoft Point-to-Point Encryption)によるデータ暗号化を行うかどうかを設定します。VPNサーバーのセキュリティポリシーに合わせて設定します。データ暗号化を有効にする場合はチェックを付けます。有効にした場合の暗号化強度は、40bitまたは128bitがVPNサーバー設定により自動的に選択されます。
DNS検索ドメイン	追加の検索ドメインをドメイン名で入力します。設定しない場合は空白のままにします。

■ L2TP VPN設定

L2TP VPNの追加をタップしたときは、次のような画面が表示されます。



次の表に従って値を設定します。

項目名	説明
VPN名	このVPN構成の任意の名称を設定します。
VPNサーバーの設定	VPNサーバーのFQDNまたはIPアドレスを設定します。
L2TPセキュリティ保護を有効にする	L2TP のトンネル認証を行うかどうかを設定します。VPNサーバーの認証設定に合わせて設定します。トンネル認証を有効にする場合はチェックを付けます。
L2TPセキュリティ保護を設定する	「L2TPセキュリティ保護を有効にする」とした場合に値を設定します。L2TP トンネル認証の事前共有鍵(shared secret)を設定します。VPNサーバーで定義されているトンネル認証のための事前共有鍵(shared secret)と同じ文字列を設定します。
DNS検索ドメイン	追加の検索ドメインをドメイン名で入力します。設定しない場合は空白のままにします。

■ L2TP/IPSec PSK VPN設定

L2TP/IPSec PSK VPNの追加をタップしたときは、次のような画面が表示されます。



次の表に従って値を設定します。

項目名	説明
VPN名	このVPN構成の任意の名称を設定します。
VPNサーバーの設定	VPNサーバーのFQDNまたはIPアドレスを設定します。
IPSec事前共有鍵の設定	IPSecの認証(IKE SA)のための事前共有鍵(pre-shared key)を設定します。VPNサーバーで定義されている機器認証のための事前共有鍵と同じ文字列を設定します。
L2TPセキュリティ保護を有効にする	L2TP のトンネル認証を行うかどうかを設定します。VPNサーバーの認証設定に合わせて設定します。トンネル認証を有効にする場合はチェックを付けます。

項目名	説明
L2TPセキュリティ保護を設定する	「L2TPセキュリティ保護を有効にする」とした場合に値を設定します。L2TP トンネル認証の事前共有鍵(shared secret)を設定します。VPNサーバーで定義されているトンネル認証のための事前共有鍵(shared secret)と同じ文字列を設定します。
DNS検索ドメイン	追加の検索ドメインをドメイン名で入力します。設定しない場合は空白のままにします。

■ L2TP/IPSec CRT VPN設定

L2TP/IPSec CRT VPNの追加をタップしたときは、次のような画面が表示されます。
L2TP/IPSec CRT VPN設定の場合、事前にmicroSDカードなどから証明書のインストールを行う必要があります。



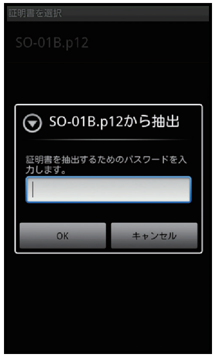
次の表に従って値を設定します。

項目名	説明
VPN名	このVPN構成の任意の名称を設定します。
VPNサーバーの設定	VPNサーバーのFQDNまたはIPアドレスを設定します。
L2TPセキュリティ保護を有効にする	L2TP のトンネル認証を行うかどうかを設定します。VPNサーバーの認証設定に合わせて設定します。トンネル認証を有効にする場合はチェックを付けます。
L2TPセキュリティ保護を設定する	「L2TPセキュリティ保護を有効にする」とした場合に値を設定します。L2TP トンネル認証の事前共有鍵(shared secret)を設定します。VPNサーバーで定義されているトンネル認証のための事前共有鍵(shared secret)と同じ文字列を設定します。
証明書を設定する	証明書の設定を行います。 設定したVPNサーバーに対応する証明書の設定を行ってください。

項目名	説明
CA証明書を設定する	CA証明書の設定を行います。 設定したVPNサーバーに対応するCA証明書の設定を行ってください。
DNS検索ドメイン	追加の検索ドメインをドメイン名で入力します。設定しない場合は空白のままにします。

（参考）証明書のmicroSDカードからのインストールについて

L2TP/IPSec CRT VPN設定で証明書を設定する場合、microSDカードのルートフォルダにサーバー管理者から提供された「.p12」ファイルを格納した上で、インストールを行う必要があります。
インストールは、「設定」→「現在地情報とセキュリティ」の「SDカードからインストール」をタップします。
インストールする証明書を選択すると、パスワード設定画面が表示されますので、サーバー管理者から提供された証明書のパスワードを設定してください。
パスワード設定後に、証明書名設定画面が表示されますので証明書に任意の名称を設定してください。
設定したVPN証明書は、L2TP/IPSec CRT VPN接続の証明書の設定から選択できます。





6 を押して「保存」をタップする

VPN構成が保存され接続の準備が完了します。

途中で作成を中止する場合は、「キャンセル」をタップします。



7 VPN設定画面に作成したVPN構成が表示される

VPN構成が保存され接続の準備が完了します。

構成を変更または削除する場合は、一覧表示されているVPN名を長くタッチします。

VPN構成は複数作成することができます。



（参考）認証情報ストレージについて

L2TP VPN設定で「L2TPセキュリティ保護を有効にする」にチェックをつけて保存をタップした場合、またはL2TP/IPSec PSK VPNの追加をタップした場合は、初回のみ右のような認証情報ストレージのパスワード設定画面が表示されます。
認証情報ストレージによってL2TP VPNおよびL2TP/IPSec PSK VPNの事前共有鍵はAES 128bit CBC暗号化され、SO-01B内に保存されます。
認証情報ストレージのパスワードは、SO-01B電源オフ、または「設定」→「現在地情報とセキュリティ」の認証情報ストレージにある「安全な認証情報の使用」のチェックを外した場合に再度入力が必要となります。また、「設定」→「現在地情報とセキュリティ」→「パスワードの設定」をタップしてパスワードの変更ができ、「設定」→「現在地情報とセキュリティ」→「ストレージの消去」をタップしてパスワードの削除と認証情報ストレージ内の情報の削除ができます。



VPNの接続

VPNを構成後、以下の手順に従いVPNの接続を行います。

1　VPN設定画面で接続する「VPN名」をタップする

VPNサーバーへの接続が開始されます。



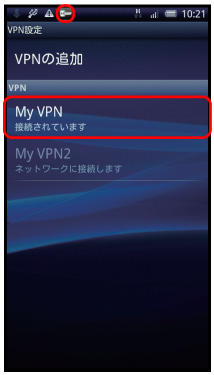
2 ユーザー認証ダイアログが表示され、「ユーザー名」と「パスワード」を入力する

VPNサーバーであらかじめ定義されたものを入力します。ユーザー名の入力を次回より省略したい場合は、「ユーザー名を保存」へチェックを入れます。



3 接続と認証が成功すると、VPN接続アイコンが通知領域に表示される

VPN名の表示が「接続されています」に変わります。



VPNの切断

VPNを切断するには以下の手順に従います。

1 通知領域を開き、VPNの通知をタップする

VPN設定画面が表示されます。



2 接続中の「VPN名」をタップする

VPNサーバーとの切断が開始されます。



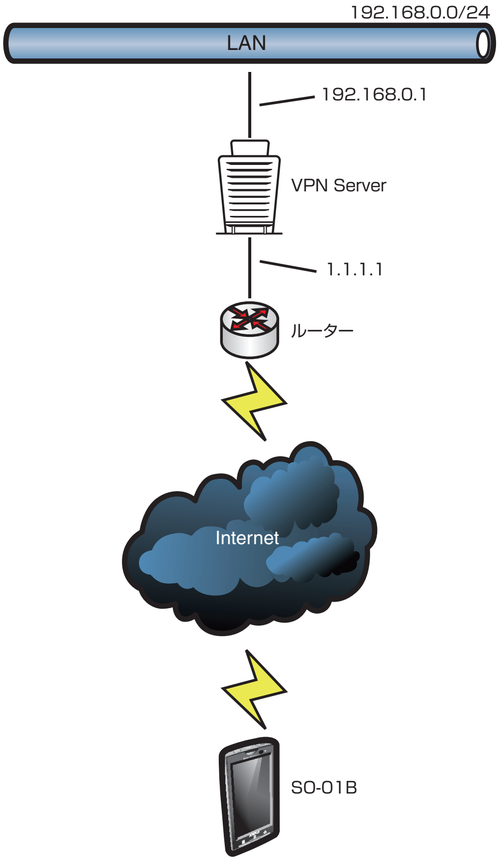
3 切断が完了されると、通知領域にVPNの通知が表示される

VPNサーバーとの切断が完了しました。



付録：VPNサーバーの設定例

ここでは、VPNサーバーの設定例として、Microsoft Windows Server 2003を用いたVPNサーバーの構成を説明します。説明の中で具体的なIPアドレスが記載されていますが、説明を分かりやすくするための例として用いていますので、実際にはVPNサーバーを設置するネットワークに準じたものを使用してください。
本構成では次のような環境を想定しています。



通信プロトコル

VPNサーバーへの通信経路にルーター・ファイアウォールが設置されている場合は、利用するVPNプロトコルに応じて、必要な通信が許可されていることを確認します。それぞれのVPNプロトコルで利用する通信プロトコルは次の通りです。

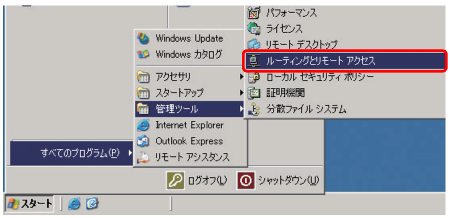
VPNプロトコル	ポート番号	プロトコル番号	備考
PPTP	1723	6/TCP	PPTP
	―	47/GRE	General Routing Encapsulation
L2TP/IPSec PSK L2TP/IPSec CRT	1701	17/UDP	L2TP
	500	17/UDP	ISAKMP
	4500	17/UDP	IPSec NAT-Traversal
	―	50/ESP	Encapsulation Security Payload

※ なおIPSecを用いないL2TPでの接続は、Windows Server 2003では標準対応していません。

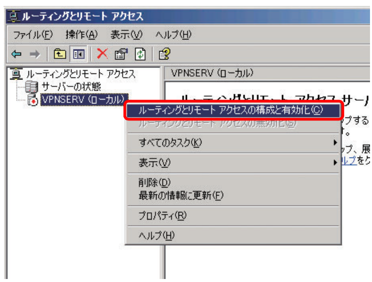
ルーティングとリモートアクセスの設定（全プロトコル共通）

VPNサーバーソフトウェアとして、Windows Server 2003へインストール済みの「ルーティングとリモートアクセス」を使用します。

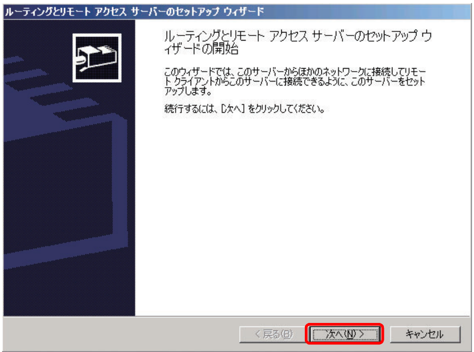
1 「スタート」→「管理ツール」→「ルーティングとリモートアクセス」をクリックする



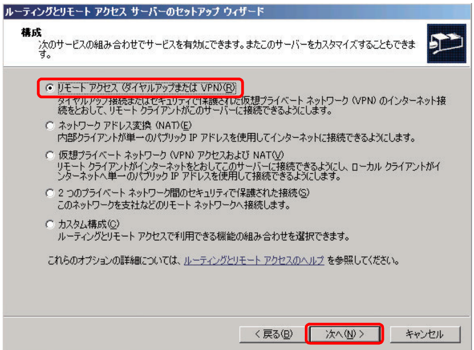
2 「(VPNサーバー名)」を右クリック →「ルーティングとリモートアクセスの構成と有効化」を選択する



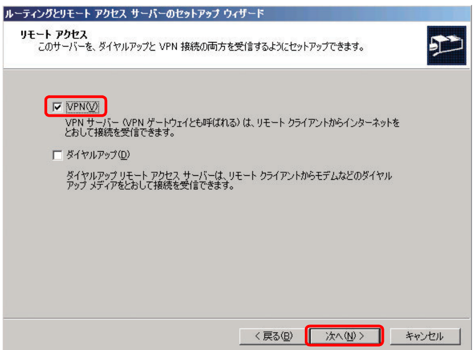
3 「ルーティングとリモートアクセスサーバーのセットアップウィザード」が起動するので、「次へ」をクリックする



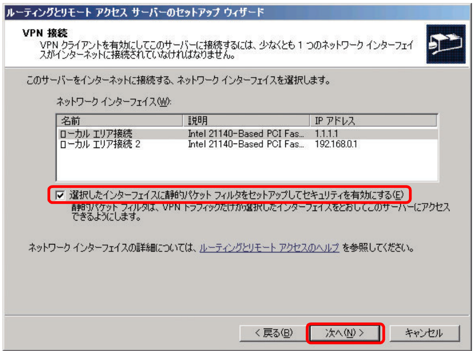
4 「リモートアクセス（ダイヤルアップまたはVPN）」を選択し、「次へ」をクリックする



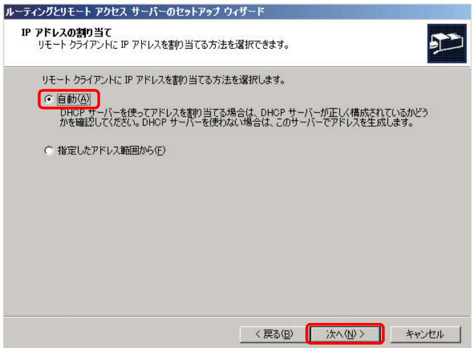
5 「VPN」を選択し、「次へ」をクリックする



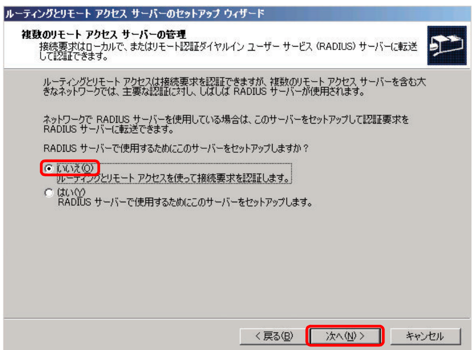
6 **インターネット側に接続されているネットワークインターフェイスとして「ローカルエリア接続」を選択し、さらに「選択したインターフェイスに静的パケットフィルタをセットアップしてセキュリティを有効にする」を選択し、「次へ」をクリックする**



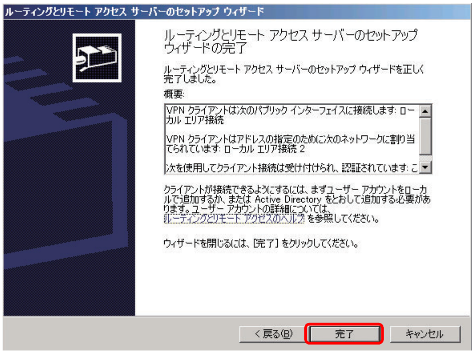
7 **「自動」を選択し、「次へ」をクリックする**



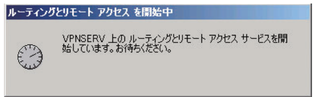
8 **本構成例ではRADIUSサーバーを使用しないため、「いいえ」を選択し、「次へ」をクリックする**



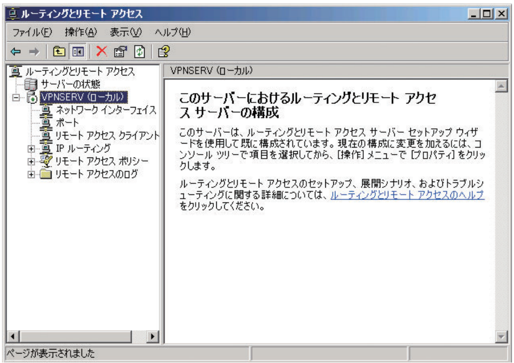
9 「完了」をクリックする



10 サービスの開始中のアニメーションウィンドウが表示されるので、しばらく待つ



11 ルーティングとリモートアクセスサービスが開始される

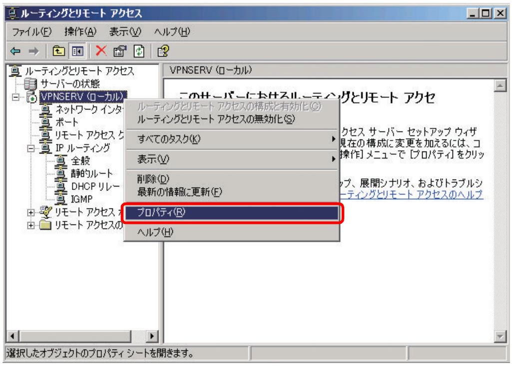


以上で、PPTPでのVPN接続が可能となりました。L2TP/IPSec PSKでのVPN接続を設定する場合は、ひきつづき次の「L2TP/IPSec PSK接続の設定」（P.20）へ進んでください。
L2TP/IPSec CRTでのVPN接続を設定する場合は、「L2TP/IPSec CRT接続の設定」（P.21）を行います。

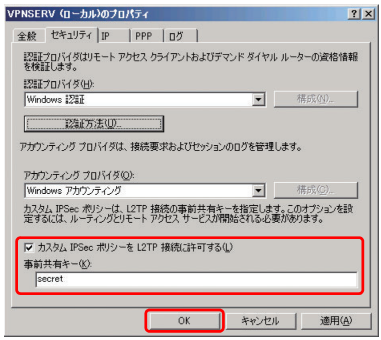
L2TP/IPSec PSK接続の設定

1 **「ルーティングとリモートアクセスの設定（全プロトコル共通）」（P.16）の設定を行う**

2 **左ペインの「ルーティングとリモートアクセス」で「(VPNサーバー名)」を右クリックし、プロパティをクリックする**



3 **「セキュリティ」タブをクリックして、「カスタムIPSecポリシーをL2TP接続に許可する」にチェックを入れ、さらに事前共有キーを入力（例：「secret」）、その後「OK」をクリックする**

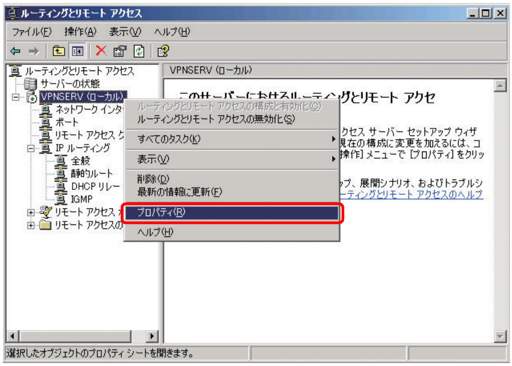


以上で、L2TP/IPSec PSKでのVPN接続設定が完了しました。

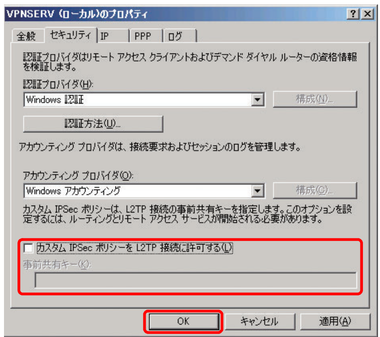
L2TP/IPSec CRT接続の設定

1 **「ルーティングとリモートアクセスの設定（全プロトコル共通）」（P.16）の設定を行う**

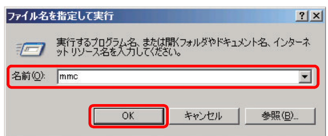
2 **左ペインの「ルーティングとリモートアクセス」で「(VPNサーバー名)」を右クリックし、プロパティをクリックする**



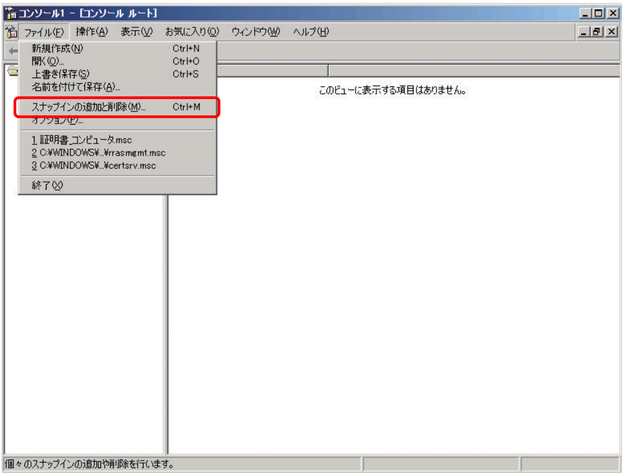
3 **「セキュリティ」タブをクリックして、「カスタムIPSecポリシーをL2TP接続に許可する」にチェックが入っていないことを確認し、「OK」をクリックする**



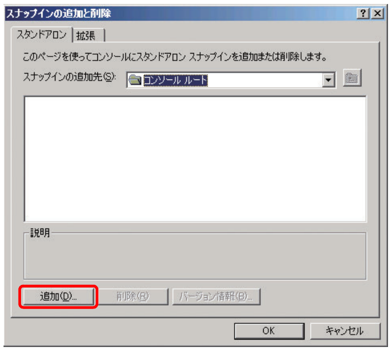
4 **「スタート」→「ファイル名を指定して実行」を開き、「mmc」と入力し、「OK」をクリックする**



5 「ファイル」→「スナップインの追加と削除」をクリックする



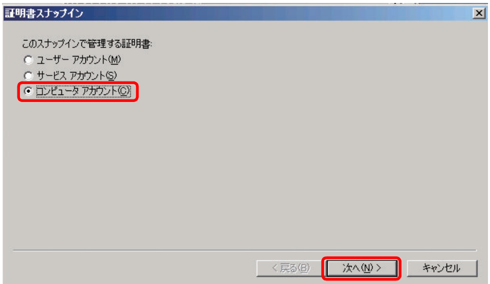
6 「追加」をクリックする



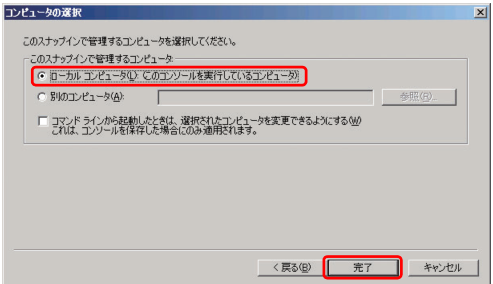
7 「証明書」を選択し、「追加」をクリックする



8 「コンピュータアカウント」を選択し、「次へ」をクリックする



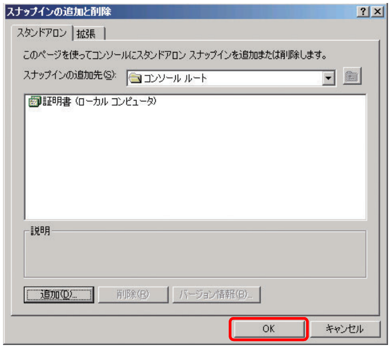
9 「ローカルコンピュータ」を選択し、「完了」をクリックする



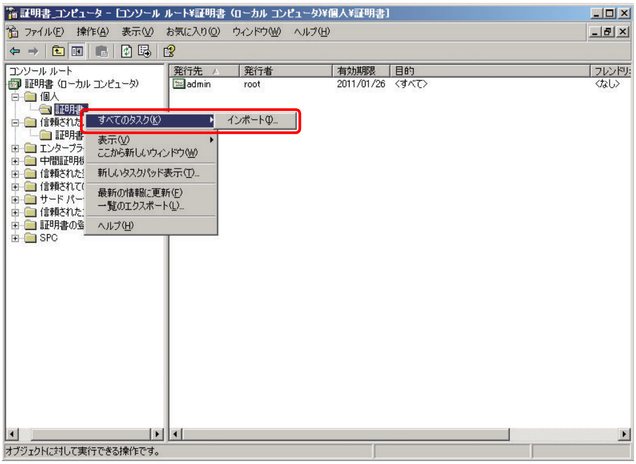
10 「閉じる」をクリックする



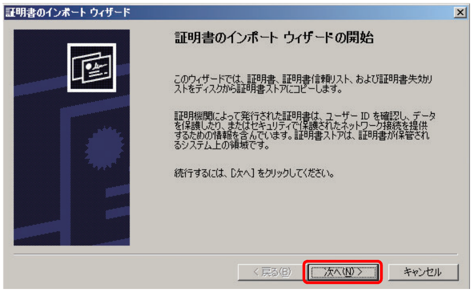
11「OK」をクリックし、画面を閉じる



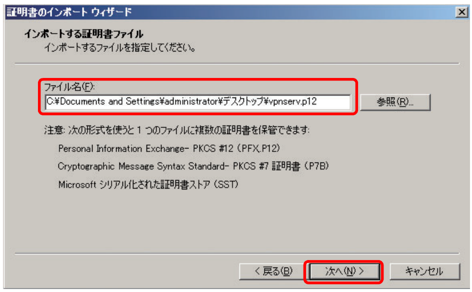
12 証明書コンソール画面上で、左ペインの「証明書（ローカルコンピュータ)」から「個人」の「証明書」を右クリックし、「すべてのタスク」→「インポート」をクリックする



13「証明書インポートウィザードの開始」画面が起動するので、「次へ」をクリックする



14 インポートするファイル（例：vpnserv.p12を選択しています）を指定し、「次へ」をクリックする

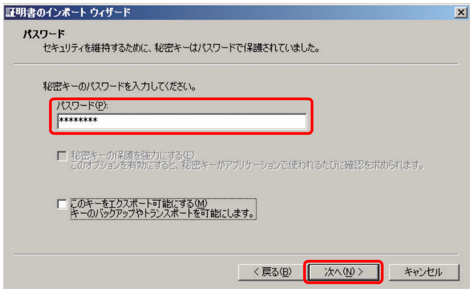


PKCS#12（Public-Key Cryptography Standard #12）形式ファイルは次のようなアイコンです。

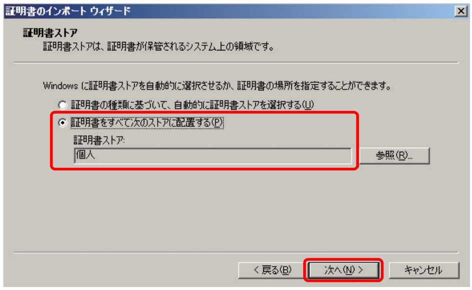


PKCS#12形式ファイルの作成方法については、「PKCS#12証明書ファイル作成方法」（P.30）を参考にしてください。

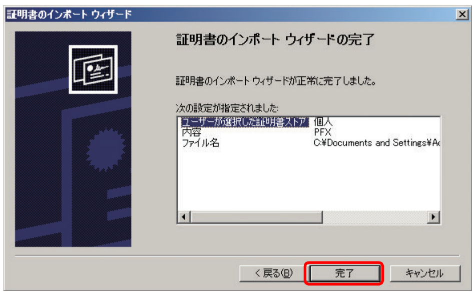
15 p12ファイルを作成するときに指定したエクスポートパスワードを指定し、「次へ」をクリックする



16 証明書ストア選択画面では、「証明書をすべて次のストアに配置する」を選択し、証明書ストアには「個人」を選択したあと、「次へ」をクリックする

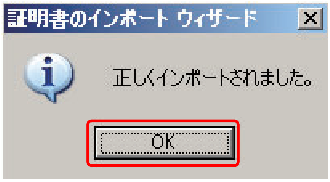


17「完了」をクリックする

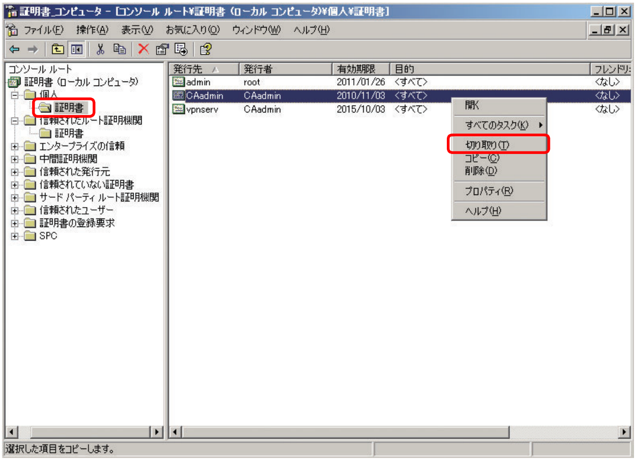


証明書インポートウィザードが完了しました。

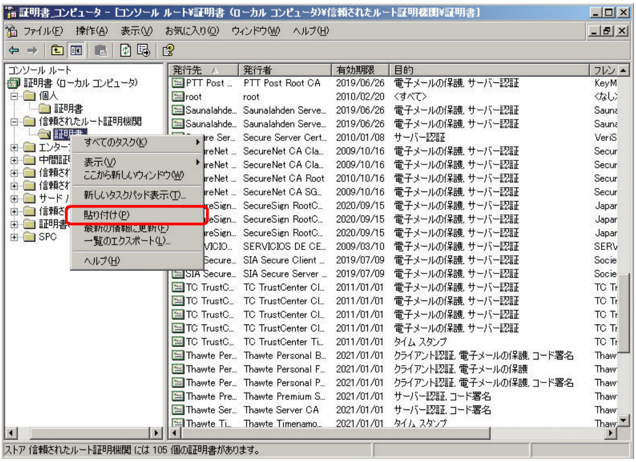
18 完了を知らせるポップアップ画面が表示されたら、「OK」をクリックする



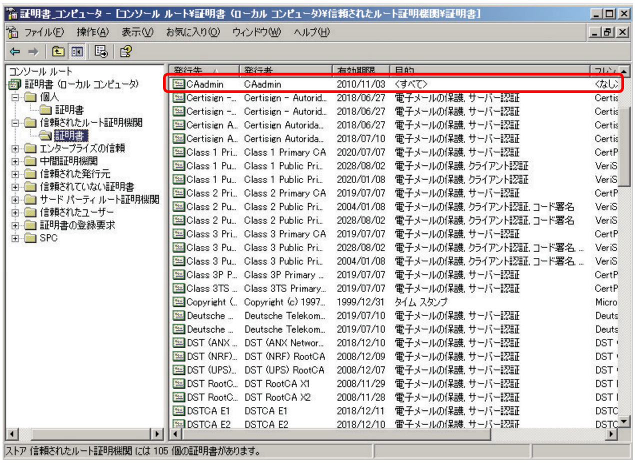
19 証明書コンソール上で、左ペインの「証明書（ローカルコンピュータ)」から「個人」の「証明書」を選択し、右ペイン内のルート証明書（例では、「CAadmin」がルート証明書、「vpnserv」がVPNサーバー用の証明書となっています）を右クリックし、「切り取り」をクリックする



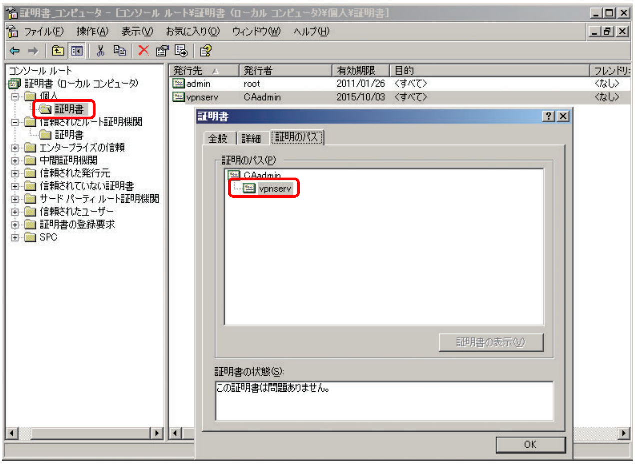
20 左ペインの「証明書（ローカルコンピュータ）」から「信頼されたルート証明機関」の「証明書」を右クリックし、「貼り付け」をクリックする



21 右ペインにルート証明書が追加されたことを確認する（例：「CAadmin」）



22 **左ペインの「証明書（ローカルコンピュータ)」から「個人」の「証明書」を選択し、サーバー用の証明書（例：「vpnserv」）をダブルクリックし、「証明書のパス」タブをクリックし、サーバー用の証明書が有効となっていることを確認する**



以上でL2TP/IPSec CRTでのVPN接続設定が完了しました。

PKCS#12証明書ファイル作成方法

PKCS#12（Public-Key Cryptography Standard #12）証明書ファイルは、証明書、秘密鍵、ルート証明書など必要となる複数のファイルを一つのファイル内のチェーンに格納することができ、配布が容易です。ここでは、OpenSSLを利用したPKCS#12証明書ファイルの作成方法を説明します。OpenSSLの各コマンド内で指定されているパラメータは一例となっていますので、社内のセキュリティポリシーなど、ご利用の環境に適した値を入力してください。
また、ここではVPNサーバー用の証明書ファイルの作成方法の説明となっていますが、SO-01Bへインポートする証明書も同様の方法で作成することができます。その場合は、説明文内のファイル名vpnserv.key, vpnserv.csr, vpnserv.pem, vpnserv.p12などを、別のファイル名（SO-01B.key, SO-01B.csr, SO-01B.pem, SO-01B.p12など）で作成してください。

■ OpenSSLのインストールとCA認証局の設定

OpenSSLのインストールとCA認証局の設定を行います。詳細については、
OpenSSL公式サイトhttp://www.openssl.org/
を参考にしてください。

■ 秘密鍵の作成

秘密鍵ファイルvpnserv.keyを作成します。次のようなコマンドを実行します。（RSA 1024bitの例）

```
openssl genrsa -out vpnserv.key 1024
```

■ CSRの作成

CSRファイルvpnserv.csrを作成します。次のようなコマンドを実行します。（有効期限を365日間とする例）

```
openssl req -new -day 365 -key vpnserv.key -out vpnserv.csr
```

■ CAの署名

CSRファイルに基づきCAにて署名された証明書ファイルvpnserv.pemを作成します。次のようなコマンドを実行します。

```
openssl ca -config <path to openssl.cfg> -in vpnserv.csr -out vpnserv.pem
```

<path to openssl.cfg> は、opensslのコンフィグファイルopenssl.cfgまたはopenssl.cnfのパスに置き換えてください。

■ PKCS#12ファイルの作成

秘密鍵、署名済みの証明書、CA証明書が統合されたPKCS#12証明書ファイルを作成します。次のようなコマンドを実行します。

```
openssl pkcs12 -export -in vpnserv.pem -inkey vpnserv.key -certfile <path to CACertFile> -out vpnserv.p12
```

<path to CACertFile> は、CAの証明書ファイルのパスを指定してください。
なお、エクスポートパスワードが空白の場合、SO-01Bへインポートできないことがありますので、適宜設定してください。

- 参考URL
  - VPNサーバーとファイアウォールの構成
    http://technet.microsoft.com/ja-jp/library/cc737500(WS.10).aspx
  - データの暗号化
    http://technet.microsoft.com/ja-jp/library/cc785633(WS.10).aspx
  - 認証プロトコルと認証方法
    http://technet.microsoft.com/ja-jp/library/cc738300(WS.10).aspx
  - トンネリング プロトコル
    http://technet.microsoft.com/ja-jp/library/cc786069(WS.10).aspx
  - パケット フィルタを管理する
    http://technet.microsoft.com/ja-jp/library/cc784616(WS.10).aspx
  - コンピュータの証明書を管理する
    http://technet.microsoft.com/ja-jp/library/cc780916(v=WS.10).aspx
  - OpenSSL: The Open Source toolkit for SSL/TLS
    http://www.openssl.org/